

REMARKS

Claims 2-25 were previously pending in this application with claims 2, 8, 13, 18, 22, 23, 24, and 25 being independent claims. No new matter has been added.

Please amend the Attorney Docket Number from 212515 to MS# 177765.01.

Rejection of Claims 2-12, 22, and 23

Claims 2, 8, 9, 22, and 23 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,092,201 to Turnbull [hereinafter Turnbull] in view of U.S. Patent No. 6,748,530 to Aoki [hereinafter Aoki]. Applicant respectfully responds to the rejection as follows:

Turnbull is directed towards extending secure communication operations via shared lists. More particularly, Turnbull describes an authorized user creating a shared list containing secure communication parameters of an end user, such as the public key certificate of the end-user or a certification authority. To authenticate the shared list, the authorized user signs the list. Others, even those not contained within the list, may access the shared list to obtain the certificates of the users contained in the list. (See, Turnbull, Abstract). In this manner, the accessing user may validate the list with the public key of the authorized user and validate the public key certificate of the end-user using a certification authority. The accessing user may use the public encryption keys in the certificates of the list to encrypt a messages directly or used to wrap a session key to communicate with those in the list. (See, Turnbull, Col. 6, lines 40-46).

Aoki is directed toward a certification process using a responsible person of a group to generate and authenticate a certificate for a new member of a group. More particularly, an individual or group temporarily registers identifying information at a server. (See, Aoki, Col. 8, lines 39-54). The responsible person of a group selects the

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

temporary registration and may confirm the association of the identifying information and the selected individual/group. (See, Aoki, Col. 8, lines 55– 60). The responsible person then generates an individual certificate by signing the identifying information and public key of the individual with the responsible person private key; or in the case of a group, the responsible person may generate a group certificate by signing the identifying information and public key of the new group's responsible person with a private key of the responsible person of a hierarchically higher group or with a responsible person's group private key. (See, Aoki, Col. 10, lines 5–41 and Col. 18, lines 8–13). Thereafter, the individual or group may authorize the group to include its information in a group list. (See, Aoki, Col. 18, lines 14–17 and FIG. 33).

Claim 2

Independent claim 2 recites, *inter alia*, forming by a first member of the group, a group membership certificate containing the peer's public key and signed with a group private key of a group public/private key pair. Applicant agrees with the Examiner's statement that "Turnbull does not teach signing with a group public/private key pair." However, the cited reference of Aoki does not cure this deficiency in Turnbull. More particularly, the group public/private key of the cited section of Aoki is used to sign a certificate of an entering group, and not of an individual entering a group.

The Examiner's motivation to combine the teachings of Aoki with Turnbull are stated as "Aoki teaches a simplified certification apparatus and method that can be performed uniformly and fairly within its own group without necessitating the external 3rd party such as CA (Certification Authority)." However, as noted above, Turnbull does not teach or suggest a certificate for a group, but rather a shared listing of multiple certificates to allow extended secure communications. More particularly, there is nothing in Turnbull that suggests the need or desire for a group key for a shared list of certificates, and there is nothing in Aoki which suggests that the certification of a group

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

can be used in a shared list for extended secure communications, as shown in Turnbull. Moreover, the mere inclusion of the group public/private key of Aoki in Turnbull does not implement the stated motivation of a certification process which removes the necessity for a certification authority. More particularly, signing a shared list of Turnbull with a group key rather than the authorized user private key does not allow an accessing user to avoid certifying the certificates of the shared list through a certification authority. Thus, there is no motivation to combine Turnbull with Aoki, and accordingly, Applicant respectfully requests withdrawal of the rejection under § 103.

Moreover, even if Aoki showed using a group private key to sign a shared list, the combination of a group private key with Turnbull does not teach or suggest the features of claim 2. More particularly, a combination of Turnbull and Aoki does not teach or suggest sending the group certificate to the peer to *invite* the peer to join the group, the group membership certificate allowing the peer to join the group through a second member other than the first member as claimed in claim 2. The shared list of Turnbull is used not to enter a group, but rather, to save encryption schemes for a list of users to be used in sending other communications. There is no invitation to a peer to join a group in Turnbull.

The Examiner suggests that Turnbull teaches the features of claim 2, by suggesting "the invitation of the user 2 by the user 1 to join the group is interpreted based on the situation that the originating user 1 would also be required to be authenticated by the invited user 2 via validating the originating user's signature." (*Office Action*, page 3). However, Turnbull does not teach or suggest that the user 2 added to the list validates the originating user at all. Rather, a separate user accessing the list may validate the signature of the originating user 1, the authorized user of Turnbull. The 'invited' user 2 added to the shared list does not validate anything to be added to the list.

Type of Response: Amendment after FINAL
Application Number: 09/955,924
Attorney Docket Number: 177765.01
Filing Date: 09/19/2001

Moreover, even if Turnbull taught validation of the originating user 1, such a teaching does not teach or suggest the features of claim 2. More particularly, validation of the originating user 1 by an 'invited' user 2 (to use the language suggested by the Examiner), does not teach or suggest the group membership certificate allowing the peer to join the group through a second member other than the first member. Validation by the invited user 2 of the same originating user 1 does not teach or suggest allowing the peer to join the group through a second member *other than the first member*. In the Examiner's suggested interpretation, there is no joining of the group through a second member other than the first member (assumed by the Examiner to be the originating user 1). The invited user 2, doing the validation in the Examiner's suggested interpretation, is not a member of the group other than the first member, as recited in claim 2. Thus, Turnbull in view of Aoki does not teach or suggest the features of claim 2.

Claim 2 also recites, *inter alia*, a method of inviting and joining a peer to a secure peer-to-peer group. The primary reference of Turnbull does not teach or suggest inviting and joining a peer to a secure peer-to-peer group. Rather, Turnbull suggests creating a shared list of certificates to extend secure communications between users, which are not described as peers. Rather, as shown in Figure 1 of Turnbull, the end-users are connected to a server/manager 24 and a certification authority 22, both which indicate that the end-users of Turnbull are not peers. The shared list of user encryption codes of Turnbull does not create a group among peers. Even if such a shared list were a peer-to-peer group, Turnbull does not invite members to the list; rather, the authorized user of Turnbull adds users to the list.

Applicant assumes that the Examiner is suggesting a modification of Turnbull in view of common knowledge. However, no motivation for such modification is provided. Thus, Applicant respectfully requests that the Examiner cite a reference in support of his

Type of Response: Amendment after FINAL
Application Number: 09/955,924
Attorney Docket Number: 177765.01
Filing Date: 09/19/2001

position as required in M.P.E.P. § 2144.03, or if the Examiner is relying upon facts within his personal knowledge, to file an affidavit establishing those facts pursuant to § 2144.03. Here, claim 2 is directed specifically toward inviting a peer to a secure peer-to-peer group, which is also the basis for the Examiner's reliance on common knowledge. Accordingly, it appears that the Examiner is relying on common knowledge to reject the principle basis of claim 2, in direct contravention to the guidelines in M.P.E.P. § 2144.03. Thus, the motivation for modifying the shared list of Turnbull to incorporate a peer-to-peer group is without foundation in the prior art of record, which is respectfully believed to render the rejection improper under M.P.E.P. § 2144.03.

Accordingly, claim 2 patentably distinguishes over Turnbull in view of Aoki such that the rejection under § 103 should be withdrawn. Claims 3-7 depend from independent claim 2, and are patentable for at least the foregoing reasons.

Claim 22

Claim 22 recites a computer-readable medium having computer executable instructions for performing the steps of claim 2. Accordingly, claim 22 is patentable for at least the foregoing reasons.

Claim 8

Claim 8 recites, *inter alia*, forming by the first member a first group membership certificate containing the peer's public key (P_{U1}) and a second group certificate signed with the group private key (K_G), the first group membership certificate being signed with a private key of the first member (K_{U2}). As noted above with respect to claim 2, Applicant agrees with the Examiner's statement that "Turnbull does not teach signing with a group public/private key pair." However, as noted above with respect to claim 2, the cited reference of Aoki does not cure these deficiencies in Turnbull. More particularly, the group public/private key of the cited section of Aoki is used to sign a certificate of an entering group, and not of an individual entering a group.

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

In addition, as noted above with respect to claim 2, there is no motivation to combine Aoki and Turnbull. Specifically, there is nothing in Turnbull that suggests the need or desire for a group key for a shared list of certificates, and there is nothing in Aoki which suggests that the certification of a group can be used in a shared list for extended secure communications, as shown in Turnbull. Moreover, as noted above with respect to claim 2, the mere inclusion of the group public/private key of Aoki in Turnbull does not implement the stated motivation of a certification process which removes the necessity for a certification authority. Thus, there is no motivation to combine Turnbull with Aoki, and accordingly, Applicant respectfully requests withdrawal of the rejection under § 103.

In addition, as noted above with respect to claim 2, the Examiner suggests that rather than signing the shared list with the authorized user's private key, the group key of Aoki should be used. However, even if this combination were supported by the cited references and the stated motivation, there is no teaching or suggestion that a first group membership certificate be signed by the private key of the first member and that a second group membership certificate be signed by the group private key. More particularly, if the cited combination of Turnbull and Aoki teaches that the group private key of Aoki may be used both *in place of* the authorized person's private key (as suggested in rejecting claim 2), then the same cited combination of Turnbull and Aoki cannot teach or suggest that the group private key of Aoki be used *in addition to* the authorized person's private key (as suggested in rejecting claim 8). Thus, the combination of Turnbull and Aoki does not teach or suggest the features of claim 8.

Even if Aoki showed using a group private key to sign a shared list in addition to a signature by the authorized person, the combination of a group private key with Turnbull does not teach or suggest the features of claim 8. More particularly, a combination of Turnbull and Aoki does not teach or suggest sending the first and

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

second group certificates from the first member to the peer to *invite* the peer to join the group as claimed in claim 8. The shared list of Turnbull is used not to enter a group, but rather, to save encryption schemes for a list of users to be used in sending other communications. There is no invitation to a peer to join the list in Turnbull.

The Examiner suggests that Turnbull teaches the features of claim 8 by suggesting "the invitation of the user 2 by the user 1 to join the group is interpreted based on the situation that the originating user 1 would also be required to be authenticated by the invited user 2 via validating the originating user's signature." (*Office Action*, page 3). However, as noted above with respect to claim 2, Turnbull does not teach or suggest that the user 2 added to the list validates the originating user at all. Rather, a separate user accessing the list may validate the signature of the originating user 1, the authorized user of Turnbull. Thus, Turnbull in view of Aoki does not teach or suggest the features of claim 8.

Claim 8 also recites, *inter alia*, in a secure peer-to-peer group having a predefined public/private key pair (P_G/K_G), a method of inviting a peer to join the group. The primary reference of Turnbull does not teach or suggest inviting a peer to a secure peer-to-peer group. Rather, as noted above with respect to claim 2, Turnbull suggests creating a shared list of certificates to extend secure communications between users, which are not described as peers. The shared list of user encryption codes of Turnbull does not create a group among peers. Even if such a shared list were a peer-to-peer group, Turnbull does not invite members to the list; rather, the authorized user of Turnbull adds users to the list.

Applicant assumes that the Examiner is suggesting a modification of Turnbull in view of common knowledge. However, no motivation for such modification is provided. Thus, the motivation for modifying the shared list of Turnbull to incorporate a peer-to-

Type of Response: Amendment after FINAL
Application Number: 09/955,924
Attorney Docket Number: 177765.01
Filing Date: 09/19/2001

peer group is without foundation in the prior art of record, which is respectfully believed to render the rejection improper under M.P.E.P. § 2144.03.

Accordingly, claim 8 patentably distinguishes over Turnbull and Aoki such that the rejection under § 103 should be withdrawn. Claims 9–12 depend from independent claim 8, and are patentable for at least the foregoing reasons.

Claim 9

Claim 9 recites, *inter alia*, the method of claim 8 wherein the step of forming by the first member comprises the step of forming a group membership certificate having a structure $((P_{U1})K_G)K_{U2}$. The Examiner suggests that Turnbull may be interpreted such that “the originating user [1] (i.e., the issuer) should also be required to be authenticated by the invited user [2] via validating the originating user’s signature (i.e., using the additional the [sic] issuer’s signature which is signed with K_{U2} in addition to $((P_{U1})K_G)$ ” and cites Turnbull Col. 6, lines 20–23. (See, Office Action, page 4, 1st parag.).

Initially, Applicant assumes that the Examiner mistakenly switched the nomenclature of his suggested interpretation of Turnbull. Specifically, with respect to claim 2, the Examiner called the issuing user as user 1, and called the invited user as user 2. Applicant will continue with the nomenclature begun in the discussion of claim 2 and cited in the brackets within the Examiner’s quotation above.

The Examiner seems to suggest an interpretation of a combination of Turnbull and Aoki as having the issuer’s signature in addition to the signature by the group private key) However, as noted above with respect tot claim 2, the Examiner is already asserting that the group private key of Aoki *replaces* the issuing user’s private key signature. Thus, Applicant is unable to determine how the same combination can teach the group key of Aoki as replacing and being in addition to the issuing user’s private key. Moreover, even if the combination of Turnbull and Aoki were to teach a group key

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

signature in addition to the issuing user's signature, there is nothing in Aoki and Turnbull which teaches or suggests the order of the signatures as recited in claim 9.

Accordingly, claim 9 patentably distinguishes over Turnbull and Aoki such that the rejection under § 103 should be withdrawn.

Claim 23

Claim 23 recites a computer-readable medium having computer executable instructions for performing the steps of claim 8. Accordingly, claim 23 is patentable for at least the foregoing reasons.

Rejection of claim 13-21, 24 and 25

Claims 13-15, 17, 18, 20, 21, 24 and 25 stand rejected under 35 U.S.C. § 103(a) as being obvious over Turnbull in view of U.S. Patent No. 6,266,420 to Langford et al. [hereinafter Langford]. Applicant respectfully traverses the rejection as follows:

Claim 13

Independent claim 13 recites, *inter alia*, receiving a group invitation from a first member containing an invitation certificate having a group ID provided therein and resolving the group ID to find a third member of the group different from the first member. The cited section of Turnbull, i.e., Col. 7 line 2-12, does not teach or suggest resolving the group ID to find a third member of the group. Specifically, the Examiner suggests an interpretation of Turnbull that the shared list is a functional group ID and the another user in the group other than the issuer/creator/owner can also be authorized to modify the shared list and provide the modified list to other users via the same process as the original issuer. However, to resolve the function group ID identified by the Examiner as the shared list, the 'invited' per must have access to the contents of the shared list; and to get such access, the 'invited' peer must be an authorized member, and not just an invited member. Thus, the shared list of Turnbull is not a group invitation as recited in claim 13. In addition, the Examiner's suggested

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

interpretation suggests that a third user may be authorized to modify the shared list, but such interpretation does not teach or suggest that the 'invited' peer can access the identification of the third peer nor that the 'invited' peer has the modification abilities. Thus, Turnbull does not teach or suggest these features of claim 13.

Independent claim 13 also recites, *inter alia*, sending a connect message to the third member containing the invitation certificate signed with the private key. In this manner, claim 13 recites that the connect message to the *third member other than the first member* includes the invitation certificate that is signed by a private key of the peer. The cited section of Turnbull (Col. 6 lines 20–23) does not teach or suggest these features of claim 13. Specifically, the cited section of Turnbull is validation of the originating user's signature by a user accessing the list, and does not teach or suggest that the user accessing the list is the 'invited' user, nor that the accessing user sends this list to a third member identified in the list. In this manner, claim 13 distinguishes over Turnbull, and thus, Applicant respectfully requests that the rejection under § 103 be withdrawn.

Independent claim 13 also recites, *inter alia*, receiving an accept message from the third member containing a group membership certificate signed by a private key of the third member. The Examiner cites section of Turnbull, i.e., col. 6 lines 20–23, and col. 7, lines 28–29) as suggesting an "ACCEPT" message from the user 2. However, Applicant is unable to find anywhere in the cited sections of Turnbull any reference to an accept message sent by a *third member* other than the first member, much less an accept message which contains a group certificate, which is separate from the invitation certificate sent to the invited member by the first member as recited in claim 13. Since Turnbull does not teach or suggest the recited features of claim 13, Applicant respectfully requests that the rejection under § 103 be withdrawn.

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

Applicant agrees with the Examiner that Turnbull does not teach or suggest receiving a group shared key to enable decryption of group traffic as recited in claim 13. However, the Examiner erroneously suggests that Langford, teaching a group communication process, may be combined with the shared list of Turnbull. Specifically, the Examiner states the motivation to combine as "providing an effective secure group communication that substantially reduces the data overhead accompanying each secure message in comparison to using the security credentials of each member." However, such teaching by Langford and the stated motivation by the Examiner directly teaches away from a combination of Langford with Turnbull. Turnbull suggests exactly the communication method rejected by Langford. More particularly, as noted above, the accessing user of Turnbull may use the individual public encryption keys in the certificates of the list to encrypt a messages directly or used to wrap a session key to communicate with those in the list. In contrast, the communication method of Langford suggests using a session key to encrypt a message, and wrapping the session key with a group key. See, Langford, col. 3, lines 14-22). Thus, Langford teaches away from using a shred list of Turnbull, and thus, should not be combined with Turnbull.

Since Turnbull in view of Langford does not teach or suggest all of the features of claim 13, claim 13 patentably distinguishes over Turnbull in view of Langford such that the rejection under § 103 should be withdrawn. Claims 14-17 depend from independent claim 13, and are patentable for at least the foregoing reasons.

Claim 24

Claim 24 recites a computer-readable medium having computer executable instructions for performing the steps of claim 13. Accordingly, claim 24 is patentable for at least the foregoing reasons.

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

Claim 18

Independent claim 18 recites, *inter alia*, receiving at a first member of the peer-to-peer group, a connect message from the peer containing an invitation certificate generated by a second member of the peer-to-peer group and signed by a private key of the peer. The cited sections of Turnbull do not teach or suggest receiving a connect message from an 'invited' peer, the connect message containing an invitation certificate generated by a second member of the peer-to-peer group and signed by the private key of the invited peer. Rather, as noted above with respect to claim 13, Turnbull suggests that the shared list is not an invitation certificate. Moreover, the 'invited' member does not send the shared list, even were it an invitation certificate, rather, an authorized member of the group can only send the shared list. Thus, Turnbull does not teach or suggest these features of claim 18.

Independent claim 18 also recites, *inter alia*, sending an accept message to the peer. The Examiner cites section of Turnbull, i.e., col. 6 lines 20-23, and col. 7, lines 28-29) as suggesting an "ACCEPT" message from the user 2. However, Applicant is unable to find anywhere in the cited sections of Turnbull any reference to an accept message sent by a *first member* other than the second member. Since Turnbull does not teach or suggest the recited features of claim 18, Applicant respectfully requests that the rejection under § 103 be withdrawn.

Applicant agrees with the Examiner that Turnbull does not teach or suggest sending a group shared key to the peer as recited in claim 18. However, the Examiner erroneously suggests that Langford, teaching a group communication process, may be combined with the shared list of Turnbull. Specifically, as noted above with respect to claim 13, "providing an effective secure group communication that substantially reduces the data overhead accompanying each secure message in comparison to using the security credentials of each member", as taught by Langford and provided as motivation

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

to combine directly teaches away from a combination of Langford with Turnbull. Turnbull suggests exactly the communication method rejected by Langford. Thus, Langford teaches away from using a shred list of Turnbull, and thus, should not be combined with Turnbull.

Since Turnbull in view of Langford does not teach or suggest all of the features of claim 18, claim 18 patentably distinguishes over Turnbull in view of Langford such that the rejection under § 103 should be withdrawn. Claims 19-21 depend from independent claim 18, and are patentable for at least the foregoing reasons.

Claim 25

Claim 25 recites a computer-readable medium having computer executable instructions for performing the steps of claim 18. Accordingly, claim 25 is patentable for at least the foregoing reasons.

CONCLUSION

Accordingly, in view of the above amendment and remarks it is submitted that the claims are patentably distinct over the prior art and that all the rejections to the claims have been overcome. Reconsideration and reexamination of the above Application is requested. Based on the foregoing, Applicants respectfully requests that the pending claims be allowed, and that a timely Notice of Allowance be issued in this case. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not

Type of Response: Amendment after FINAL
Application Number: 09/955,924
Attorney Docket Number: 177765.01
Filing Date: 09/19/2001

covered by an enclosed check please charge any deficiency to Deposit Account No. 50-0463.

Respectfully submitted,
Microsoft Corporation

Date: 7/11/05

By: 


Carole A Boelitz, Reg. No. 48,958
Attorney for Applicants
Direct telephone (425) 722-6035
Microsoft Corporation
One Microsoft Way
Redmond WA 98052-6399

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

- deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450
- transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) 872-9306.

7/11/05
Date


Carole A Boelitz

Type of Response: Amendment after FINAL
Application Number: 09/955,924
Attorney Docket Number: 177765.01
Filing Date: 09/19/2001